剰余体$K[x]/〈f〉$における逆冪計算 (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

田島, 慎一

CITATION:

田島, 慎一. 剰余体$K[x]/〈f〉$における逆冪計算 (Computer Algebra : Design of Algorithms, Implementations and Applications). 数理解析研究所講究録 2006, 1514: 171-175

ISSUE DATE:

2006-09

URL:

http://hdl.handle.net/2433/58665

数理解析研究所講究録
1514巻 2006年 171-175

剰余体 $K[x]/\langle f\rangle$ における逆冪計算

田島慎一
SHINICHI TAJIMA
新潟大学工学部情報工学科
NIIGATA UNIVERSITY*

論文 [1], [3], [4], [5] 等において, 一変数有理関数の部分分数分解, 留数計算, 極におけるローラン展開, 一変数剰余公式を求める新たな方法を与えた. これらの計算法はいずれも, ある種の代数的局所コホモロジーが満たす一階の微分方程式系を考え, その微分方程式の解を逐次構成していく事で問題を解くという共通した構造を持っている. これら逐次計算の初項等は, 既約多項式が定める剰余体での逆冪計算により与えることができる. そこで本稿では, 剰余体における逆冪計算を効率的に行う方法について考える.

1. 逆冪計算の問題点.

有理数体 Q を K とおき, 一変数有理数係数多項式全体のなす環を $K[x]$ で表す. 既約な多項式 $f(x)\in K[x]$ が多項式環 $K[x]$ において生成するイデアルを $\langle f\rangle$ で表す. いま, f で割り切れないような多項式 $g(x)$ と自然数 m が与えられたとする. これらに対し, 条件

$$c(x)g(x)^m = 1 \bmod f$$

をみたす多項式 $c(x)$ を効率的に求める方法について考える. 多項式 $c(x)$ の次数は $\deg c < \deg f$ を満たすとしてよい.

自然数 m は比較的大きな数であることを想定しているので, $c(x)$ の各項の係数となる有理数は分母・分子ともにかなりの桁数となる. そのため, 拡張ユークリッドアルゴリズムを多項式 $f(x), g(x)^m$ の組に対し直接適用して $c(x)$ を求めることは, 計算効率に問題がある. そこで本稿では, まず拡張ユークリッドの互除法により

$$b(x)g(x) = 1 \bmod f$$

なる多項式 $b(x)$ を求め, $c(x) = b(x)^m \bmod f$ により $c(x)$ を計算することを考える.

さて, 有理数係数の多項式計算を数式処理を用いて行う際は, なるたけ整数係数の多項式の計算に帰着させていくのが計算効率化の常套手段である. いまの場合, 有理数係数多項式 $b(x)$ の各項の係数に現れる有理数の共通分母を D とおき, $B(x)$ を $B(x) = Db(x)$ で定めれば $B(x)$ は, 明らかに $b(x) = \frac{B(x)}{D}$ をみたす整数係数多項式となる. ここで,

$$b(x)^m = \frac{B(x)^m}{D^m} \bmod f$$

が成り立つので, 問題が右辺の分子 $B(x)^m \bmod f$ の計算に帰着されたことになり, あとは m の2進展開を用いたべき計算と f による擬剰余を組み合わせれば, 有理数係数多項式のベキ計算が整数係数多項式の計算で効率よく実行できる. と言いたいところだが以下に見る様に, この計算法にはかなり無駄がある.

*tajima@ie.niigata-u.ac.jp

例 $f(x)=x^4+5x^3-7x^2+2x-17, g(x)=f'(x)$ とおく.
このとき, $b(x)f'(x)=1 \bmod f$ なる $b(x)\in K[x]$ は,

$$b(x)=\frac{-10498x^3-13375x^2+319727x-89317}{15739503}$$

で与えられる. 計算すると,

$$\begin{aligned}
b^2(x) &= \frac{843x^3+4838x^2-3360x-4258}{15739503} \bmod f,\\
b^3(x) &= \frac{118062014x^3+306297920x^2-1898600065x+4923104282}{24773195467009} \bmod f,\\
b^4(x) &= \frac{7374845x^3-29153037x^2+1074799x+12991668}{24773195467009} \bmod f
\end{aligned}$$

を得る. ここで, $D=15739503$ とおくと $D^2=24773195467009$ となるので, $b^3(x) \bmod f$, $b^4(x) \bmod f$ の分母は D^3, D^4 ではなく, D^2 で与えられる.

例 (庄司卓夢) $f(x)=x^4+x^3+x^2+x+1, g(x)=f'(x)$ とおく.
$b(x)g(x)=1 \bmod f$ を満たす多項式 $b(x)$ およびそのベキをいくつか計算してみると

$$\begin{aligned}
b(x) &= \frac{1}{5}(x^2-x) \bmod f,\\
b(x)^2 &= \frac{1}{25}(-3x^3-x-1) \bmod f,\\
b(x)^3 &= \frac{1}{125}(-4x^3-3x^2-2x-6) \bmod f,\\
b(x)^4 &= \frac{1}{125}(-x^2+x-1) \bmod f,\\
b(x)^5 &= \frac{1}{625}(3x^3-x^2+2x+1) \bmod f,\\
b(x)^6 &= \frac{1}{3125}(7x^3+3x^2+3x+7) \bmod f,
\end{aligned}$$

等を得る. 分母に注目すると, $D=5$ のベキ $D, D^2, D^3, D^3, D^4, D^5$ が並んでいることがわかるが, $b(x)$ のベキとの関係はさきほどの例とはことなることが見て取れる.

これらの例が示すように, $b^m(x) \bmod f$ の係数を整数化するのに D^m を用いるとかなりの無駄が生じることになる. 従って, 剰余体 $K[x]/\langle f\rangle$ における $g(x)$ の逆冪を効率的に求める為には, $B(x)^m \bmod f$ を求めてから D^m で割るという前述の方法によらない別の計算法を考える必要がある.

2. 最小多項式の利用.

有理数係数の一変数多項式環を $K[x]$ で表す. 既約多項式 $f(x)\in K[x]$ が生成するイデアルを $\langle f\rangle \subset K[x]$ で表し, $K[x]$ の $\langle f\rangle$ による剰余を $K[x]/\langle f\rangle$ で表す. 与えられた多項式 $g(x)\in K[x]$ に対し, $b(x)g(x)=1 \bmod f$ なる $b(x)\in K[x]$ が $K[x]/\langle f\rangle$ において定める剰余類を v で表す. ここで, v の最小多項式を考え, それを $\chi(v)$ とおく. 最小多項式 χ の次数を $d=\deg\chi$ とおくと, $\chi(v)$ は $d-1$ 次以下の次数の多項式 $\psi(v)$ を用いて

$$\chi(v)=v^d-\psi(v)$$

と表せるとしてよい.

いま, v を不定元とする一変数有理数係数多項式環を $K[v]$ で表し, 多項式 $\chi(v)$ が生成するイデアル $\langle\chi\rangle$ による $K[v]$ の剰余を $K[v]/\langle\chi\rangle$ で表す. 多項式 v^d が $K[v]/\langle\chi\rangle$ において定める剰余類を w で表すことにする. この時,

$$\begin{aligned} w = v^d &= \psi(v) \bmod \chi, \\ w^2 = v^{2d} &= \psi(v)^2 \bmod \chi, \\ w^4 = v^{4d} &= (\psi(v)^2 \bmod \chi)^2 \bmod \chi, \\ w^8 = v^{8d} &= ((\psi(v)^2 \bmod \chi)^2 \bmod \chi)^2 \bmod \chi, \end{aligned}$$

等が成り立つ事に注意しよう. 一般に, $v^{qd} \bmod \chi = w^q$ を求めるには q の2進展開

$$q = q_0 + q_1 \times 2 + q_2 \times 2^2 + \cdots + q_s \times 2^s$$

を用いて $w^q = w^{q_0}(w^2)^{q_1}(w^4)^{q_2}\cdots(w^{2^s})^{q_s}$ と変形し, χ による剰余を取りながら右辺の積を計算する事で, 高々 $d-1$ 次の多項式 ψ_q による表現 $w^q = \psi_q(v)$ を求めることができる.

さて, 準備が整ったので, 以下に, $b(x)^m \bmod f$ の計算法を与えよう. まず, $u = g(x) \bmod$ とおき, $u \in K[x]/\langle f\rangle$ の最小多項式をもとめ,

$$a_0 + a_1 u + a_2 u^2 + \cdots + a_d u^d$$

とおく. この時, v の最小多項式 $\chi(v)$ は,

$$\chi(v) = a_d + a_{d-1} v + \cdots + a_1 v^{d-1} + a_0 v^d$$

で与えられる.

次に, 自然数 m を d で割り, 商と余りを求めそれらをそれぞれ q, r とおく. このとき, $m = qd + r$ より, $v^m = (v^d)^q \cdot v^r$ を得るが, $w = v^d$ であるので, q の2進展開を利用して $w^q = \psi_q(v)$ なる ψ_q を求める. 更に $v^r\psi_q(v)$ を $\chi(v)$ で割った余りを求め, それを

$$\phi(v) = p_0 + p_1 v + p_2 v^2 + \cdots + p_\ell v^\ell$$

とおけば, $v^m = \phi(v) \in K[v]/\langle\chi\rangle$ なる表現を得る. ここで $\ell < d$ となることを注意しておく. さて, $\chi(b(x)) = 0 \bmod f$ が成り立つことから, 明らかに

$$b(x)^m = \phi(b(x)) \bmod f$$

が従うが, $b(x)g(x) = 1 \bmod f$ より,

$$\phi(b(x)) = (p_0 g(x)^\ell + p_1 g(x)^{\ell-1} + \cdots + p_{\ell-1} g(x) + p_\ell) b(x)^\ell \bmod f$$

と書き換える事が出来る. 従って, $b(x)^m \bmod f$ を求めるには, ホーナー法等により

$$p_0 g(x)^\ell + p_1 g(x)^{\ell-1} + \cdots + p_{\ell-1} g(x) + p_\ell \bmod f,$$

を求め, $b(x)^\ell \bmod f$ との積をとった後, 再び f による剰余をとれば良い事になる. 最小多項式 χ を利用することで, 逆冪の計算をかなり効率化することができた.

実際にプログラムを書く時は, 有理数係数多項式の計算をなるたけ整数係数多項式の計算で置き換えるように工夫したりすることで, 計算の効率化を図ることができる.

3. 具体例

$f(x)=x^3+5x^2-4x-17, g(x)=f'(x)=3x^2+10x-4$ とする. このとき,
$b(x)g(x)=1 \bmod f$ なる多項式 $b(x)$ は,

$$b(x)=\frac{74x^2+237x-419}{7473},$$

で与えられる.

最小多項式を用いることで $b(x)^{12} \bmod f$ を計算してみる. まず, $u=g(x) \bmod f \in K[x]/\langle f\rangle$ の最小多項式を求めると $7473-37u^2+u^3$ となるので, $v=b(x) \bmod f \in K[x]/\langle f\rangle$ の最小多項式

$$\chi(v)=7473v^3-37v+1$$

を得る.

補足 最小多項式 $\chi(v)$ の不定元 v に $b(x)$ を代入し, $\chi(b(x))$ を計算すると

$$\frac{405224x^6+3893436x^5+5586186x^4-30778479x^3+52090965x^2+59293134x+98139589}{55845729}$$

を得る. この 6 次式を $f(x)$ で割るとあまりが零となり, $f(x)$ で割り切れることが確かめられる. この式からも, 最小多項式を利用することで計算の効率化が図れることが見て取れる.

次に, 最小多項式 χ による剰余計算を行い,

$$\begin{aligned} v^3 &= \frac{1}{7473}(37v-1) \bmod \chi, \\ v^6 &= \frac{1}{(7473)^2}((37v-1)^2) \bmod \chi, \\ v^{12} &= \frac{1}{(7473)^5}(130727179v^2-10476809v+210085) \bmod \chi \end{aligned}$$

等を得る. ここで, v^{12} に注目する.

$$130727179-10476809g(x)+210085g(x)^2=-23657282x^2-768267785x+229567450 \bmod f$$

と

$$b(x)^2=\frac{-3x^2-10x+41}{7473} \bmod f$$

を用いると,

$$b(x)^{12}=\frac{1}{(7473)^6}(-1167465403x^2-3790275523x+11319562515) \bmod f$$

を得る.

4. まとめ

最小多項式を用いることで, 剰余体における逆冪計算の効率化が図れることを示した. 本稿で述べた計算法を数式処理システム Risa/Asir([2]) に実装し計算所用時間等を計測したところ, 従来のものに比べかなり計算効率が良いものであることが確かめられた. 留数計算アルゴリズム ([3]) 等では f' 等の逆冪計算が必要となるが, その計算に本提案アルゴリズムを用いることで更なる効率化が可能となる.

参 考 文 献

[1] 加藤涼香, 田島慎一: 有理関数のローラン展開アルゴリズムと代数的局所コホモロジー, 京都大学数理解析研究所講究録 **1395**「Computer Algebra」(2004), 50–56.

[2] M. Noro, T. Shimoyama, and T. Takeshima: Asir User's Manual, 2005.

[3] 庄司卓夢, 田島慎一: 高速留数計算アルゴリズム, 京都大学数理解析研究所講究録 **1456**「Computer Algebra」(2005), 133–143.

[4] 庄司卓夢, 田島慎一: 多項式剰余公式の計算アルゴリズム, 京都大学数理解析研究所講究録「Computer Algebra」掲載予定.

[5] 田島慎一: 一変数留数計算アルゴリズムについて, 京都大学数理解析研究所講究録 「積分核の代数解析的研究」, 掲載予定.